CLAIMS

WHAT IS CLAIMED IS:

1. An integrated circuit, comprising:

a first bus interface logic for coupling to a first external bus;

a microcontroller configured to receive an input from a security device over a direct input different from the first external bus, wherein the microcontroller is further configured to receive a request and to query the security device over the direct input.

2. The integrated circuit of claim 1, further comprising:

a second external bus interface logic for coupling to a second external bus, wherein the microcontroller is further configured as a remote management engine, wherein the microcontroller is further configured to receive management sensor data over the second external bus.

3. The integrated circuit of claim 2, further comprising:

a first internal bus, wherein data from the second external bus is routable by the remote management engine over the first internal bus.

4. The integrated circuit of claim 3, further comprising:

an embedded Ethernet controller coupled to the first internal bus.

5. The integrated circuit of claim 4, wherein the embedded Ethernet controller is configured to route management sensor data to an external management server.

6. The integrated circuit of claim 2, wherein the remote management engine comprises an Alert Standard Format management engine.

7. The integrated circuit of claim 6, wherein the management data comprises Alert Standard Format sensor data.

8. The integrated circuit of claim 1, wherein the request is received from an external processor.

9. The integrated circuit of claim 1, wherein the integrated circuit comprises a bridge, wherein the bridge further comprises:

a third bus interface logic for coupling to a second external bus.

10. The integrated circuit of claim 9, wherein the bridge comprises a south bridge, wherein the second external bus is configurable as a second input/output bus.

11. The integrated circuit of claim 1, further comprising:

a register configured to store data exchanged between the microcontroller and an external processor.

12. The integrated circuit of claim 11, wherein the microcontroller is further configured to read the data from the register in response to the request.

13. An integrated circuit, comprising:

a first interface means for coupling to a first external communications means;

a controller means coupled to the first external communications means, wherein the controller means is configured to receive an input from a security means over a direct input means different from the first external communications means, wherein the controller means is further configured to receive a request and to query the security means over the direct input means.

14. The integrated circuit of claim 13, further comprising:

a second external interface means for coupling to a second external communications means, wherein the controller means is further configured as a remote management engine, wherein the controller means is further configured to receive management data over the second external communications means.

15. The integrated circuit of claim 14, further comprising:

a first internal communications means, wherein data from the second external communications means is routable by the remote management engine over the first internal communications means.

16. The integrated circuit of claim 15, further comprising:

an embedded Ethernet means coupled to the first internal communications means.

17. The integrated circuit of claim 16, wherein the embedded Ethernet means is configured to route management data to an external management means.

18. The integrated circuit of claim 14, wherein the remote management engine comprises an Alert Standard Format management engine.

19. The integrated circuit of claim 18, wherein the management data comprises Alert Standard Format sensor data.

20. The integrated circuit of claim 13, wherein the request is received from an external processing means.

21. The integrated circuit of claim 13, wherein the integrated circuit comprises a bridge, wherein the bridge further comprises:

a third interface means for coupling to a second external communications means.

22. The integrated circuit of claim 21, wherein the bridge comprises a south bridge, wherein the second external communications means is configurable as a second input/output communications means.

23. The integrated circuit of claim 13, further comprising:

a storage means configure to store data exchanged between the controller means and an external processing means.

24. The integrated circuit of claim 23, wherein the controller means is further configured to read the data from the storage means in response to the request.

25. A computer system, comprising:

a first external bus; and

an integrated circuit, the integrated circuit comprising:

a first bus interface logic for coupling to the first external bus;

a microcontroller coupled to the first external bus, wherein the microcontroller is configured to receive an input from a security device over a direct input different from the first external bus, wherein the microcontroller is further configured to receive a request and to query the security device over the direct input.

26. The computer system of claim 25, further comprising:

a second external bus, wherein the microcontroller is further configured as a remote management engine, wherein the microcontroller is further configured to receive management data over the second external bus.

27. The computer system of claim 26, with the integrated circuit further comprising:

a first internal bus; and

a second bus interface logic for coupling to a first internal bus, wherein data from the second external bus is routable by the remote management engine over the first internal bus.

28. The computer system of claim 25, with the integrated circuit further comprising:

an embedded Ethernet controller coupled to the first internal bus.

29. The computer system of claim 25, wherein the remote management engine comprises an Alert Standard Format management engine.

30. The computer system of claim 29, wherein the management data comprises Alert Standard Format sensor data.

31. The computer system of claim 28, wherein the embedded Ethernet controller is configured to route management data to the external management server.

32. The computer system of claim 25, further comprising:

a processor configured to provide the request.

33. The computer system of claim 25, further comprising:

a second external bus, wherein the integrated circuit comprises a bridge, wherein the bridge further comprises:

a third bus interface logic for coupling to a second external bus.

34. The computer system of claim 33, wherein the bridge comprises a south bridge, wherein the second external bus is configurable as a second input/output bus.

35. The computer system of claim 25, further comprising:

a processor, wherein the integrated circuit further comprises:

a register configure to store data exchanged between the microcontroller and the processor.

36. The computer system of claim 35, wherein the microcontroller is further configured to read the data from the register in response to the request.

37. The computer system of claim 25, wherein the security device includes at least one of a biometric device and a smart card reader.

38. The computer system of claim 37, wherein the biometric device is configured to accept biometric data taken from the group consisting of: a fingerprint or thumbprint, hand geometry, voiceprint, retinal scan, facial scan, body odor, ear shape, DNA profile, keystroke dynamics, pen stroke dynamics, and vein checking.

39. A computer system, comprising:

a first external communications means; and

an integrated circuit, the integrated circuit comprising:

a first interface means for coupling to the first external communications means;

a controller means coupled to the first external communications means, wherein the controller means is configured to receive an input from a security means over a direct input means different from the first external communications means, wherein the controller means is further configured to receive a request and to query the security means over the direct input.

40. The computer system of claim 39, further comprising:

a second external communications means, wherein the controller means is further configured as a remote management engine, wherein the controller means is further configured to receive management data over the second external communications means.

41. The computer system of claim 40, with the integrated circuit further comprising:

a first internal communications means; and

a second bus interface means for coupling to a first internal communications means, wherein data from the second external communications means is routable by the remote management engine over the first internal communications means.

42. The computer system of claim 39, with the integrated circuit further comprising:

an embedded Ethernet means coupled to the first internal communications means.

43. The computer system of claim 42, wherein the embedded Ethernet means is configured to route management data to the external management means.

44. The computer system of claim 39, further comprising:

a processing means configured to provide the request.

45. The computer system of claim 39, further comprising:

a second external communications means, wherein the integrated circuit comprises a bridge, wherein the bridge further comprises:

a third interface means for coupling to a second external communications means.

46. The computer system of claim 45, wherein the bridge comprises a south bridge, wherein the second external communications means is configurable as a second input/output communications means.

47. The computer system of claim 39, further comprising:

a processor, wherein the integrated circuit further comprises:

a storage means configure to store data exchanged between the controller means and the processing means.

48. The computer system of claim 47, wherein the controller means is further configured to read the data from the storage means in response to the request.

49. The computer system of claim 39, wherein the security means includes at least one of a biometric means and a smart card means.

50. The computer system of claim 49, wherein the biometric means is configured to accept biometric data taken from the group consisting of: a fingerprint or thumbprint, hand geometry, voiceprint, retinal scan, facial scan, body odor, ear shape, DNA profile, keystroke dynamics, pen stroke dynamics, and vein checking.

51. A method of operating an computer system, the method comprising:

receiving a request for an authentication, at a microcontroller;

requesting security data from a security device;

receiving the security data from the security device, at the microcontroller;

evaluating the security data; and

approving the authentication if the security data is evaluated as acceptable.

52. The method of claim 51, further comprising:

disapproving the authentication if the security data is evaluated as unacceptable.

53. The method of claim 51, wherein evaluating the security data comprises requesting an indication of acceptability inside SMM.

54. The method of claim 51, wherein requesting security data from a security device comprises requesting the security data from the security device over a direct connection between the security device and the microcontroller; and

wherein receiving the security data from the security device, at the microcontroller, comprises receiving the security data from the security device over the direct connection to the microcontroller.

55. The method of claim 51, wherein requesting security data from a security device comprises requesting biometric data from a biometric device; wherein receiving the security data from the security device, at the microcontroller, comprises receiving the biometric data from the biometric device, at the microcontroller; wherein evaluating the security data comprises evaluating the biometric data; and wherein approving the authentication if the security data is evaluated as acceptable comprises approving the authentication if the biometric data is evaluated as acceptable.

56. A method of operating an computer system, the method comprising the steps of:

receiving a request for an authentication, at a microcontroller;

requesting security data from a security device;

receiving the security data from the security device, at the microcontroller;

evaluating the security data; and

approving the authentication if the security data is evaluated as acceptable.

57. The method of claim 56, further comprising the step of:

disapproving the authentication if the security data is evaluated as unacceptable.

58. The method of claim 56, wherein the step of evaluating the security data comprises the step of requesting an indication of acceptability inside SMM.

59. The method of claim 56, wherein the step of requesting security data from a security device comprises the step of requesting the security data from the security device over a direct connection between the security device and the microcontroller; and

wherein the step of receiving the security data from the security device, at the microcontroller, comprises the step of receiving the security data from the security device over the direct connection to the microcontroller.

60. The method of claim 56, wherein the step of requesting security data from a security device comprises the step of requesting biometric data from a biometric device; wherein the step of receiving the security data from the security device, at the microcontroller, comprises the step of receiving the biometric data from the biometric device, at the microcontroller; wherein the step of evaluating the security data comprises the step of evaluating the biometric data; and wherein the step of approving the authentication if the security data is evaluated as acceptable comprises the step of approving the authentication if the biometric data is evaluated as acceptable.

61. A computer readable medium encoded with instructions that, when executed by a computer system, performs a method for operating the computer system, the method comprising:

receiving a request for an authentication, at a microcontroller;

requesting security data from a security device;

receiving the security data from the security device, at the microcontroller;

evaluating the security data; and

approving the authentication if the security data is evaluated as acceptable.

62. The computer readable medium of claim 61, the method further comprising:

disapproving the authentication if the security data is evaluated as unacceptable.

63. The computer readable medium of claim 61, wherein evaluating the security data comprises requesting an indication of acceptability inside SMM.

64. The computer readable medium of claim 61, wherein requesting security data from a security device comprises requesting the security data from the security device over a direct connection between the security device and the microcontroller; and

wherein receiving the security data from the security device, at the microcontroller, comprises receiving the security data from the security device over the direct connection to the microcontroller.

65. The computer readable medium of claim 61, wherein requesting security data from a security device comprises requesting biometric data from a biometric device; wherein receiving the security data from the security device, at the microcontroller, comprises receiving the biometric data from the biometric device, at the microcontroller; wherein evaluating the security data comprises evaluating the biometric data; and wherein approving the authentication if the security data is evaluated as acceptable comprises approving the authentication if the biometric data is evaluated as acceptable.